

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*INFORMATION ASSOCIATED WITH FACEBOOK USER ID
100007660200170 THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK, INC.

Case No.

2:19-mj-385

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 875(c)

Communicating a threat in interstate

The application is based on these facts:

See Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

May 14, 2019

City and state:

Columbus, Ohio

Applicant's signature

Bryan G. Thompson Task Force Officer

Printed name and title

Judge's signature

Kimberly A. Jolson, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

**IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK USER ID 100007660200170
THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK, INC.**

Misc. No. 2:19-mj-385

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Bryan C. Thompson, being a duly sworn police officer and Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), Cincinnati Field Office (CFO), Columbus, Ohio hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook user IDs that are stored at premises owned, maintained, controlled, or operated by Facebook, Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, further described in Section I of Attachment B, pertaining to the subscriber or customer associated with the user ID. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the information described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. I am a Police Detective with The Ohio State University Police Division and have worked for the division for 19 years since January of 2000. I am currently assigned to the FBI Joint Terrorism Task Force (JTTF), where I have been a case agent or co-case agent for several International and Domestic Terrorism investigations for the past three years. During that time, I have received specialized training in International, Domestic Terrorism, and training related to social media information gathering.

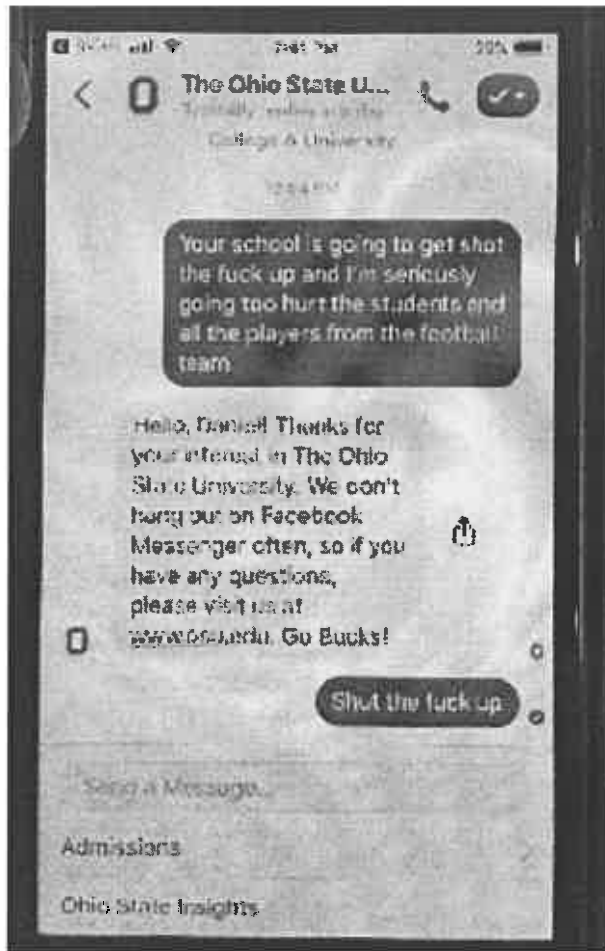
3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(c) have been committed by Daniel Lee Rippy ("Rippy"). There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

PROBABLE CAUSE

5. The FBI has been investigating Rippy regarding an internet threat sent via Facebook messenger from California to Ohio. Rippy stated he would cause serious physical harm by firearm to the patrons and athletes of The Ohio State University (OSU) football team. The threat was sent to the University's social media page, and subsequent messages were also sent to individuals, including the Head Coach and quarterback.

6. Specifically, on November 24, 2018, Rippy sent the following threat from Facebook user ID **100007660200170** to The Ohio State University Facebook messenger account:



7. The threat to the venue was first realized by an OSU Intel analyst, whose assignment was to monitor incoming social media traffic during the game. The social media thread was seen on The Ohio State University main media site that is seen by the entire university. A check of Rippy's Facebook profile suggested that Rippy was believed to be in close proximity due to the associated posts and language used to show that Rippy was actively engaged in the game and in route to or in close proximity to the Ohio State University Stadium, which prompted an enlarged presence of law enforcement officers and tactical units in an effort to thwart the incident. While efforts were being made to attempt to locate the social media profile and presence of Rippy, I was called off of my K9 assignment to assist with OSU and FBI analysts to work with Verizon

Wireless and OSU to attempt to locate the correlating phone to Rippy. While this was being done all K9 resources as well as tactical elements were given information regarding the believed appearance of Rippy and areas in where large numbers of pedestrians would congregate where a large scale attack would be probable. All units were commanded to stay in place until information was received that the units could stand down. This lasted for approximately two hours, which pushed assets past the projected end time for almost two hours.

8. An emergency cellular ping was requested by the Ohio State University Police Department, which located Rippy in Livermore, California where Livermore Police Department made contact with him. Livermore Police attempted a wellbeing check at Rippy's apartment. When contact was made, Rippy initially stated that he knew nothing about the social media posts then changed his story and stated that he did make the posts. Officers asked for consent to see his phone and the messages that he sent. Rippy complied and officers saw the Ohio State logo on the messages that he sent.

9. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

10. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

11. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

12. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

13. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or

her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

14. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

15. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

16. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

17. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

18. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

19. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

20. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

21. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

22. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

23. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may

communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

24. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook

“friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

25. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant.

28. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is “a district court of the United States ... that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Bryan C. Thompson
Task Force Officer
FBI Joint Terrorism Task Force

Subscribed and sworn to before me on May 14, 2019



Kimberly A. Jolson
UNITED STATES MAGISTRATE JUDGE

